PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-131449
(43)Date of publication of application : 19.05.1995

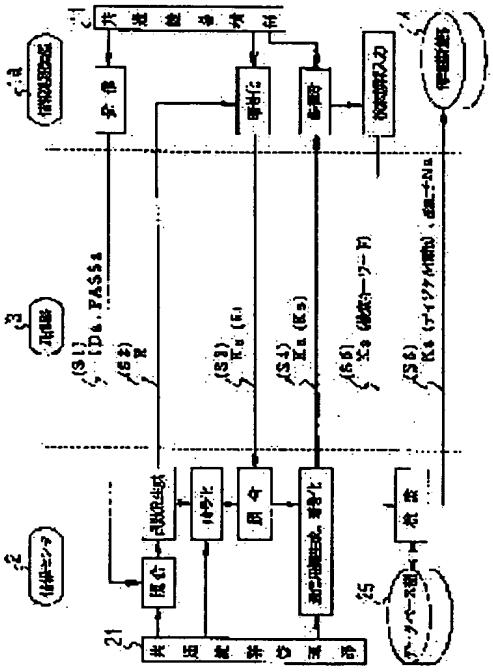
(51)Int.CI. H04L 9/00
H04L 9/10
H04L 9/12
G06F 13/00
G09C 1/00

(21)Application number : 05-275386
(22)Date of filing : 04.11.1993

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : YAMANAKA KIYOSHI

(54) DIGITAL INFORMATION COMMUNICATION SYSTEM

(57)Abstract:
PURPOSE: To provide the digital information communication system which protects information from the wrong action like wrong copy or alteration of data.
CONSTITUTION: When information is received from an information center 2 by an information processor 1a and is used, digital information to which an alteration prevention authenticator Na is given is received by communication in the cipher system using a common key Ka; and at, the time of using the information, received digital information is decoded and converted and is outputted only when it passes alteration verification by the authenticator Na. Consequently, essential intended information cannot be restored even if received digital information is copied as it is and is decoded and converted by another device or the like and is outputted, and wrong copy is prevented. Thus, the rights and profits of a writer and an information presenter are protected.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平7－131449

(43)公開日　平成７年(1995)５月19日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｈ０４Ｌ	9/00				
	9/10				
	9/12				
Ｇ０６Ｆ	13/00	３５１　Ｚ	7368－5Ｂ		
				Ｈ０４Ｌ　9/00　Ｚ	

審査請求　未請求　請求項の数４　ＯＬ　（全 15 頁）　最終頁に続く

(21)出願番号　特願平5－275386

(22)出願日　平成５年(1993)11月４日

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区内幸町一丁目１番６号

(72)発明者　山中　喜義
東京都千代田区内幸町１丁目１番６号　日本電信電話株式会社内

(74)代理人　弁理士　吉田　精孝

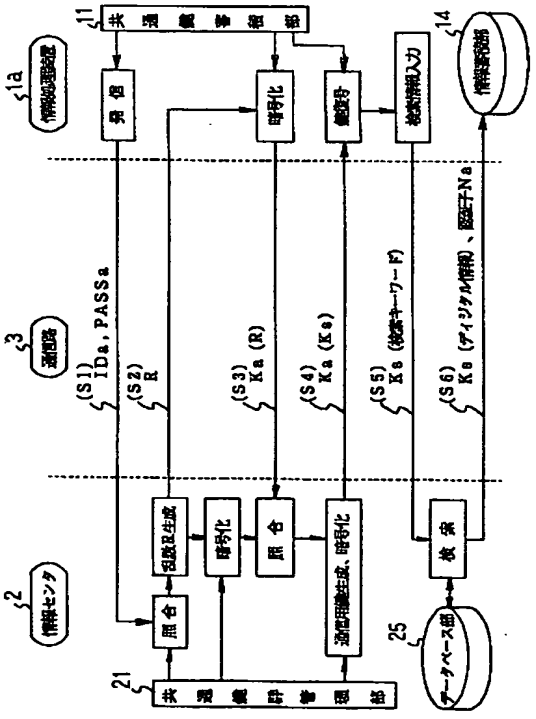
(54)【発明の名称】　ディジタル情報通信システム

(57)【要約】

【目的】　データの不正コピー、改ざん等の不正行為に対して情報を保護するディジタル情報通信システムを提供すること。

【構成】　情報センタ２から情報処理装置１ａに情報を受信して使用する際に、改ざん防止用認証子Ｎａを付与したディジタル情報を共通鍵Ｋａを用いた暗号方式の通信により受信し、利用時に認証子Ｎａにより改ざん検証して適合した場合のみ受信したディジタル情報を復号及び変換して出力する。

【効果】　受信したディジタル情報をそのままコピーして他の装置などで復号、変換出力しても、本来の意図する情報は復元されず、不正コピーを防止できる。これにより著作者並びに情報提供業者の権利及び利益を保護することができる。



【特許請求の範囲】

【請求項１】　装置番号及びパスワード並びに共通鍵を蓄積する共通鍵蓄積部と、ディジタル情報を受信制御する通信制御部と、通信開始時に装置の認証のための認証情報を作成する認証データ作成部と、受信したディジタル情報を蓄積する情報蓄積部と、ディジタル情報を復号する復号部と、該復号されたディジタル情報を所定の形態に変換して外部に出力する変換出力部とからなる情報処理装置と、

複数の情報処理装置に対応する装置番号及びパスワード並びに共通鍵群を蓄積する共通鍵群管理部と、前記情報処理装置にディジタル情報を送信制御する通信制御部と、各情報処理装置から認証情報を受信して接続可否を判定する認証部と、検索用ディジタル情報を格納するデータベース部と、該データベース部内のディジタル情報を検索する検索部と、ディジタル情報を暗号化する暗号管理部とからなる情報センタとを備え、前記情報処理装置と前記情報センタとの間でディジタル情報通信を行うディジタル情報通信システムであって、

前記情報センタに格納されているディジタル情報を前記情報処理装置に取り込むときは、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、

該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を前記情報処理装置に送信し、

該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、

該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して前記情報処理装置に送信し、

暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した検索キーワードを前記情報センタに送信し、

該検索キーワードを受信した情報センタは、該検索キーワードに基づいて前記データベース部内のディジタル情報を検索し、検索結果のディジタル情報を前記通信用暗号鍵で暗号化すると共に前記情報処理装置に対応した認証子を作成して、これらを前記情報処理装置に返送し、前記ディジタル情報及び認証子を受信した情報処理装置は、これらを前記情報蓄積部に蓄積した後、認証子の検証及びディジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力することを特徴とするディジタル情報通信システム。

【請求項２】　前記情報センタのディジタル情報を他の情報処理装置によっても利用することを前提として前記情報処理装置に取り込むときは、

前記暗号化された通信用暗号鍵を前記情報センタから受信した前記情報処理装置は、検索キーワード及びディジタル情報を利用する他の情報処理装置の装置番号を該通信用暗号鍵で暗号化して前記情報センタに送信し、

該検索キーワード及び他の情報処理装置の装置番号を受信した情報センタは、該検索キーワードに基づいて前記データベース部内のディジタル情報を検索し、検索結果のディジタル情報を前記通信用暗号鍵で暗号化すると共に前記情報処理装置に対応した認証子を作成して、これらを前記情報処理装置に返送すると同時に、前記他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記ディジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、

該他の情報処理装置に対応した通信用暗号鍵及び認証子を受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたディジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、

該複写先の他の情報処理装置は、前記認証子の検証及びディジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力することを特徴とする請求項１記載のディジタル情報通信システム。

【請求項３】　前記情報センタのディジタル情報を前記情報処理装置に取り込み通信を終了した後、該ディジタル情報を他の情報処理装置によって利用するときは、

前記情報処理装置を再度前記情報センタに接続して、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、

該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を情報処理装置に送信し、

該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、

該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して情報処理装置に送信し、

暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した前記ディジタル情報固有の情報識別番号及び前記他の情報処理装置の装置番号、並びに前記情報処理装置の共通鍵で暗号化した前記ディジタル情報受信時に使用した通信用暗号鍵を前記情報センタに送信し、

前記情報識別番号及び装置番号並びに通信用暗号鍵を受信した情報センタは、前記他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記ディジタル情

報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、
該他の情報処理装置に対応した通信用暗号鍵及び認証子を受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたディジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、
該複写先の他の情報処理装置は、前記認証子の検証及びディジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力することを特徴とする請求項１記載のディジタル情報通信システム。
【請求項４】　前記他の情報処理装置に蓄積されている前記情報センタから受信したディジタル情報を前記情報処理装置によって利用するときは、
前記情報処理装置を情報センタに接続して、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、
該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を前記情報処理装置に送信し、
該乱数を受信した前記情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、
該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して前記情報処理装置に送信し、
暗号化された通信用暗号鍵を受信した前記情報処理装置は、該通信用暗号鍵で暗号化した前記他の情報処理装置で受信したディジタル情報固有の情報識別番号、及び前記他の情報処理装置の共通鍵で暗号化した前記ディジタル情報受信時に使用した通信用暗号鍵、並びに該通信用暗号鍵で暗号化した前記他の情報処理装置の装置番号を前記情報センタに送信し、
前記情報識別番号及び装置番号並びに通信用暗号鍵を受信した情報センタは、前記情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記ディジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、
該通信用暗号鍵及び認証子を受信した情報処理装置側では、前記他の情報処理装置から前記情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたディジタル情報を複写し、
該ディジタル情報が複写された前記情報処理装置は、前記認証子の検証及び前記ディジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力することを特徴とする請求項１記載のディジタル情報通信システム。
【発明の詳細な説明】
【０００１】
【産業上の利用分野】本発明は、音楽、映像、絵画、コンピュータグラフィックス、コンピュータソフトウェア等の著作物情報をＩＳＤＮ等の通信回線によりディジタル情報として送信する際、通信に先立つ送信先の認証、通信途中での盗聴防止、並びに受信後の情報の改ざん及び不正コピーを防止し、且つ複数装置で利用を可能とする合法的コピーを許容することにより、著作権者並びに情報提供者の権利及び利益を保護するディジタル情報通信システムに関するものである。
【０００２】
【従来の技術】近年、ＩＳＤＮを代表とするディジタル通信技術及び、ディジタル情報圧縮技術（例えば、MPEG,JPEG 方式等）の発達により、音楽、絵画、映像、コンピュータソフト、コンピュータグラフィックス等の著作物をディジタル情報として通信回線利用により送信することが実現可能となってきた。例えば、コンピュータソフトウェアでは、既にパソコン通信等を利用した配送サービスを実施している例がある。今後は早晩、さらに情報量の多い音楽、映像情報等の配送サービスの出現が予想される。
【０００３】
【発明が解決しようとする課題】前述したように、ディジタル著作物の通信利用による流通が盛んになると、ディジタル情報の送信相手になりすまして通信を行ったり、或いは通信途中での盗聴等に加えて、受信した情報をディジタル形式で不正に複製して他の装置で利用する不正行為により著作権者並びに情報提供業者の権利及び利益を侵害する恐れが生じる。
【０００４】従来のパソコン通信利用によるコンピュータソフトウェア配送では、情報提供元となるセンタと接続する時に、ユーザＩＤ、パスワードによる簡易な相手確認を行う程度で通信途中での盗聴、受信後のデータの不正コピー、改ざん等の不正行為に対して防止対策が施されていなかった。
【０００５】一方、従来の不正コピー防止対策としては、フロッピーディスクの場合、標準記録方式（記録密度、セクタ、トラック数等）から一部逸脱した記録方式で記録する等して、一般のコピープログラムではリードエラーが発生する仕組みを設けている例がある。しかし、この方式では、フロッピーディスク等の記憶媒体の物理的破壊防止のためのバックアップコピーを行うことが困難になってしまう。
【０００６】また、ディジタル情報の通信利用による配送の場合、通信の効率化及び利用者拡大を図るため、著作者並びに情報提供者の権利を保護しつつ、合法的コピーを許容して、一度受信したディジタル情報を複数利用者、複数装置で利用できる仕組みは、従来のフロッピー

ディスクのコピープロテクト方式では困難であった。

【０００７】本発明の目的は上記の問題点に鑑み、データの不正コピー、改ざん等の不正行為に対して情報を保護するディジタル情報通信システムを提供することにある。

【０００８】

【課題を解決するための手段】本発明は上記の目的を達成するために、請求項１では、装置番号及びパスワード並びに共通鍵を蓄積する共通鍵蓄積部と、ディジタル情報を受信制御する通信制御部と、通信開始時に装置の認証のための認証情報を作成する認証データ作成部と、受信したディジタル情報を蓄積する情報蓄積部と、ディジタル情報を復号する復号部と、該復号されたディジタル情報を所定の形態に変換して外部に出力する変換出力部とからなる情報処理装置と、複数の情報処理装置に対応する装置番号及びパスワード並びに共通鍵群を蓄積する共通鍵群管理部と、前記情報処理装置にディジタル情報を送信制御する通信制御部と、各情報処理装置から認証情報を受信して接続可否を判定する認証部と、検索用ディジタル情報を格納するデータベース部と、該データベース部内のディジタル情報を検索する検索部と、ディジタル情報を暗号化する暗号管理部とからなる情報センタとを備え、前記情報処理装置と前記情報センタとの間でディジタル情報通信を行うディジタル情報通信システムであって、前記情報センタに格納されているディジタル情報を前記情報処理装置に取り込むときは、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を前記情報処理装置に送信し、該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して前記情報処理装置に送信し、暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した検索キーワードを前記情報センタに送信し、該検索キーワードを受信した情報センタは、該検索キーワードに基づいて前記データベース部内のディジタル情報を検索し、検索結果のディジタル情報を前記通信用暗号鍵で暗号化すると共に前記情報処理装置に対応した認証子を作成して、これらを前記情報処理装置に返送し、前記ディジタル情報及び認証子を受信した情報処理装置は、これらを前記情報蓄積部に蓄積した後、認証子の検証及びディジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力するディジタル情報通信システムを提案する。

【０００９】また、請求項２では、請求項１記載のディジタル通信システムにおいて、前記情報センタのディジタル情報を他の情報処理装置によっても利用することを前提として前記情報処理装置に取り込むときは、前記暗号化された通信用暗号鍵を前記情報センタから受信した前記情報処理装置は、検索キーワード及びディジタル情報を利用する他の情報処理装置の装置番号を該通信用暗号鍵で暗号化して前記情報センタに送信し、該検索キーワード及び他の情報処理装置の装置番号を受信した情報センタは、該検索キーワードに基づいて前記データベース部内のディジタル情報を検索し、検索結果のディジタル情報を前記通信用暗号鍵で暗号化すると共に前記情報処理装置に対応した認証子を作成して、これらを前記情報処理装置に返送すると同時に、前記他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記ディジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、該他の情報処理装置に対応した通信用暗号鍵及び認証子を受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたディジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置は、前記認証子の検証及びディジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力するディジタル情報通信システムを提案する。

【００１０】また、請求項３では、請求項１記載のディジタル通信システムにおいて、前記情報センタのディジタル情報を前記情報処理装置に取り込み通信を終了した後、該ディジタル情報を他の情報処理装置によって利用するときは、前記情報処理装置を再度前記情報センタに接続して、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を情報処理装置に送信し、該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して情報処理装置に送信し、暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した前記ディジタル情報固有の情報識別番号及び前記他の情報処理装置の装置番号、並びに前記情報処理装置の共通鍵で暗号化した前記ディジタル情報受信時に使用した通信用暗号鍵を前記情報センタに送信し、

前記情報識別番号及び装置番号並びに通信用暗号鍵を受信した情報センタは、前記他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記ディジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、該他の情報処理装置に対応した通信用暗号鍵及び認証子を受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたディジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置は、前記認証子の検証及びディジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力するディジタル情報通信システムを提案する。

【００１１】さらに、請求項４では、請求項１記載のディジタル通信システムにおいて、前記他の情報処理装置に蓄積されている前記情報センタから受信したディジタル情報を前記情報処理装置によって利用するときは、前記情報処理装置を情報センタに接続して、前記情報処理装置から前記情報センタに装置番号及びパスワードを送信し、該装置番号及びパスワードを受信した情報センタは、乱数を生成し、該乱数を前記情報処理装置に送信し、該乱数を受信した前記情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、該暗号化した乱数を受信した情報センタは、前記情報処理装置に対応した共通鍵を前記共通鍵群管理部から抽出すると共に、該共通鍵により前記送信時の乱数を暗号化し、該暗号化した乱数と前記情報処理装置から受信した暗号化された乱数とを比較し、これらの値が一致したときに、通信用暗号鍵を作成すると共に該通信用暗号鍵を前記共通鍵で暗号化して前記情報処理装置に送信し、暗号化された通信用暗号鍵を受信した前記情報処理装置は、該通信用暗号鍵で暗号化した前記他の情報処理装置で受信したディジタル情報固有の情報識別番号、及び前記他の情報処理装置の共通鍵で暗号化した前記ディジタル情報受信時に使用した通信用暗号鍵、並びに該通信用暗号鍵で暗号化した前記他の情報処理装置の装置番号を前記情報センタに送信し、前記情報識別番号及び装置番号並びに通信用暗号鍵を受信した情報センタは、前記情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記ディジタル情報に対して該共通鍵により作成された認証子を前記情報処理装置に送信し、該通信用暗号鍵及び認証子を受信した情報処理装置側では、前記他の情報処理装置から前記情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたディジタル情報を複写し、該ディジタル情報が複写された前記情報処理装置は、前記認証子の検証及び前記ディジタル情報の復号を行った後、情報内容に応じた利用形態に変換して出力するディジタル情報通信システムを提案する。

【００１２】

【作用】本発明の請求項１によれば、前記情報センタのディジタル情報を前記情報処理装置に取り込むときは、前記情報処理装置から前記情報センタに装置番号及びパスワードが送信され、該装置番号及びパスワードを受信した情報センタにおいて、乱数が生成され、該乱数が前記情報処理装置に送信される。該乱数を受信すると、前記情報処理装置は該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信し、前記情報センタにおいて、前記情報処理装置に対応した共通鍵が前記共通鍵群管理部から抽出されると共に、該共通鍵により前記送信時の乱数が暗号化され、該暗号化された乱数と前記情報処理装置から受信した暗号化された乱数とが比較され、これらの値が一致したときに、通信用暗号鍵が作成されると共に該通信用暗号鍵が前記共通鍵で暗号化されて前記情報処理装置に送信される。

【００１３】暗号化された通信用暗号鍵を受信した情報処理装置は、該通信用暗号鍵で暗号化した検索キーワードを情報センタに送信する。これにより情報センタでは、該検索キーワードに基づいて前記データベース部内のディジタル情報が検索され、検索結果のディジタル情報が前記通信用暗号鍵で暗号化されると共に前記情報処理装置に対応した認証子が作成されて、これらが情報処理装置に返送される。

【００１４】前記情報処理装置は前記情報センタからディジタル情報及び認証子を受信した後、これらを前記情報蓄積部に蓄積し、認証子の検証及びディジタル情報の復号を行ってから、情報内容に応じた利用形態に変換して出力する。

【００１５】また、請求項２によれば、前記情報センタのディジタル情報を他の情報処理装置によっても利用することを前提として前記情報処理装置に取り込む際に、前記暗号化された通信用暗号鍵を前記情報センタから受信した情報処理装置は、検索キーワード及びディジタル情報を利用する他の情報処理装置の装置番号を該通信用暗号鍵で暗号化して情報センタに送信する。これにより、該検索キーワード及び他の情報処理装置の装置番号を受信した情報センタでは、該検索キーワードに基づいて前記データベース部内のディジタル情報が検索され、検索結果のディジタル情報が前記通信用暗号鍵によって暗号化されると共に前記情報処理装置に対応した認証子が作成されて、これらが前記情報処理装置に返送される。さらにこれと同時に、前記情報センタから前記情報処理装置に対して、前記他の情報処理装置に対応する共通鍵によって暗号化された通信用暗号鍵と前記ディジタル情報に対して該共通鍵により作成された認証子が送信される。

【００１６】この後、前記情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に、前

記受信した通信用暗号鍵で暗号化されたディジタル情報及び各情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置は、前記認証子の検証及びディジタル情報の復号を行ってから、情報内容に応じた利用形態に変換して出力する。

【００１７】また、請求項３によれば、前記情報センタのディジタル情報を前記情報処理装置に取り込み通信を終了した後、該ディジタル情報を他の情報処理装置によって利用する際に、前記情報処理装置が再度前記情報センタに接続されて、前記情報処理装置から前記情報センタに装置番号及びパスワードが送信される。これにより、前記情報センタでは、乱数が生成され、該乱数が前記情報処理装置に送信される。該乱数を受信した情報処理装置は、該乱数を前記共通鍵蓄積部より抽出した共通鍵により暗号化した値を再び前記情報センタに送信する。該暗号化した乱数を受信した情報センタでは、前記情報処理装置に対応した共通鍵が前記共通鍵群管理部から抽出されると共に、該共通鍵により前記送信時の乱数が暗号化され、該暗号化された乱数と前記情報処理装置から受信した暗号化された乱数とが比較され、これらの値が一致したときに、通信用暗号鍵が作成されると共に該通信用暗号鍵が前記共通鍵で暗号化されて前記情報処理装置に送信される。

【００１８】この後、前記情報処理装置は、該通信用暗号鍵で暗号化した前記ディジタル情報固有の情報識別番号及び前記他の情報処理装置の装置番号、並びに前記情報処理装置の共通鍵で暗号化した前記ディジタル情報受信時に使用した通信用暗号鍵を前記情報センタに送信する。次いで、情報センタによって、前記他の情報処理装置に対応する共通鍵によって暗号化された通信用暗号鍵と、前記ディジタル情報に対して該共通鍵により作成された認証子が前記情報処理装置に送信される。これらを受信した情報処理装置側では、該情報処理装置から前記他の情報処理装置の情報蓄積部に対して、前記受信した通信用暗号鍵で暗号化されたディジタル情報及び他の情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵並びに各情報処理装置に対応する認証子を複写し、該複写先の他の情報処理装置では、前記認証子の検証及びディジタル情報の復号が行われ、この後情報内容に応じた利用形態に変換されて出力される。

【００１９】さらに、請求項４によれば、前記他の情報処理装置に蓄積されている前記情報センタから受信したディジタル情報を前記情報処理装置によって利用する際は、前記情報処理装置が情報センタに接続され、前記情報処理装置から前記情報センタに装置番号及びパスワードが送信される。これにより情報センタでは、乱数が生成され、該乱数が前記情報処理装置に送信される。さらに、該乱数を受信した前記情報処理装置によって、該乱数が前記共通鍵蓄積部より抽出した共通鍵により暗号化された値が再び前記情報センタに送信される。

【００２０】この後、前記情報センタによって、前記情報処理装置に対応した共通鍵が前記共通鍵群管理部から抽出されると共に、該共通鍵により前記送信時の乱数が暗号化され、該暗号化された乱数と前記情報処理装置から受信した暗号化された乱数とが比較され、これらの値が一致したときに、通信用暗号鍵が作成されると共に該通信用暗号鍵が前記共通鍵によって暗号化されて前記情報処理装置に送信される。次いで、前記情報処理装置によって、該通信用暗号鍵で暗号化された前記他の情報処理装置で受信したディジタル情報固有の情報識別番号、及び前記他の情報処理装置の共通鍵で暗号化した前記ディジタル情報受信時に使用した通信用暗号鍵、並びに該通信用暗号鍵で暗号化した前記他の情報処理装置の装置番号が情報センタに送信される。

【００２１】これらを受信した情報センタでは、前記情報処理装置に対応する共通鍵で暗号化された通信用暗号鍵と前記ディジタル情報に対して該共通鍵により作成された認証子が前記情報処理装置に送信され、該通信用暗号鍵及び認証子を受信した情報処理装置側では、前記他の情報処理装置から前記情報処理装置の情報蓄積部に、前記受信した通信用暗号鍵で暗号化されたディジタル情報を複写し、該ディジタル情報が複写された情報処理装置は、前記認証子の検証及びディジタル情報の復号を行ってから、情報内容に応じた利用形態に変換して出力する。

【００２２】

【実施例】以下、図面に基づいて本発明の一実施例を説明する。図１は、本発明の一実施例に係るディジタル情報通信システムを示す構成図である。図において、１はディジタル情報を受信し、これを蓄積して利用する情報処理装置、２はディジタル情報の提供元となる情報センタで、ディジタル情報を蓄積し、情報処理装置１からの検索要求によりディジタル情報を送信する。３は通信路で、該通信路３を介して情報センタ２と複数の情報処理装置１とが接続できるようになっている。

【００２３】情報処理装置１は、装置番号及びパスワード並びに共通鍵を蓄積する共通鍵蓄積部１１、ディジタル情報を受信制御する通信制御部１２、通信開始時に装置の認証のための認証情報を作成する認証データ作成部１３、受信したディジタル情報を蓄積する情報蓄積部１４、ディジタル情報を復号する復号部１５、及び復号されたディジタル情報を外部に例えばアナログ情報として変換出力する変換出力部１６を備え、これらはキーボード等からなる入力インタフェース部（図示せず）に接続された図示せぬ中央制御部によって動作制御されている。

【００２４】情報センタ２は、複数の情報処理装置１に対応する装置番号及びパスワード並びに共通鍵群を蓄積する共通鍵群管理部２１、情報処理装置１へのディジタ

ル情報の送信を制御する通信制御部２２、各情報処理装置１から認証情報を受信して接続可否を判定する認証部２３、ディジタル情報を検索する検索部２４、検索用ディジタル情報を格納するデータベース部２５、ディジタル情報を暗号化する暗号化部２６から構成され、これらは図示せぬ中央制御部によって動作制御されている。

【００２５】図２は、情報処理装置１内の共通鍵蓄積部１１に蓄積される情報の内容例を示す図である。図において、ＩＤａは装置番号、ＰＡＳＳａはパスワード、Ｋａは共通鍵である。

【００２６】図３は、情報センタ２内の共通鍵群管理部２１に蓄積される情報の内容例を示す図である。図において、ＩＤａ～ＩＤｃ、ＰＡＳＳａ～ＰＡＳＳｃ、Ｋａ～Ｋｃのそれぞれは、異なる情報処理装置１ａ，１ｂ，１ｃの装置番号、パスワード、共通鍵を示している。

【００２７】本実施例の処理の流れを情報処理装置１ａと情報センタ２の間での通信を例として、図１及び図４に基づいて説明する。ここで、情報処理装置１ａの構成は図１に示す情報処理装置１の構成と同等である。

【００２８】情報処理装置１ａは情報センタ２に発信して、共通鍵蓄積部１１より抽出した情報処理装置１ａの装置番号ＩＤａ及びパスワードＰＡＳＳａを情報センタ２に送信する（Ｓ１）。情報センタ２では、前記受信した装置番号ＩＤａ及びパスワードＰＡＳＳａを共通鍵群管理部２１で検索し、該装置番号ＩＤａ及びパスワードＰＡＳＳａが存在し且つこれらの組み合わせが一致した場合に、乱数Ｒを生成して情報処理装置１ａに返送する（Ｓ２）。

【００２９】情報処理装置１ａは、乱数Ｒを受信した後、認証データ作成部１３において受信した乱数Ｒを共通鍵蓄積部１１より抽出した共通鍵Ｋａによって暗号化し、暗号化した乱数Ｋａ（Ｒ）を情報センタ２に送信する（Ｓ３）。

【００３０】情報センタ２では、認証部２３において、共通鍵群管理部２１より抽出した情報処理装置１ａに対応する共通鍵Ｋａで前記乱数Ｒを暗号化すると共に、該暗号化した乱数Ｒの値と受信した暗号化乱数Ｋａ（Ｒ）の値とを照合する。この照合の結果、両者の値が一致した場合には、通信用暗号鍵Ｋｓを生成すると共に、該通信用暗号鍵Ｋｓを情報処理装置１ａに対応する共通鍵Ｋａで暗号化し、暗号化した通信用暗号鍵Ｋａ（Ｋｓ）を情報処理装置１ａに送信する（Ｓ４）。

【００３１】次に、情報処理装置１ａは暗号化した通信用暗号鍵Ｋａ（Ｋｓ）を受信した後、これを復号して通信用暗号鍵Ｋｓを復元し、検索したいディジタル情報に対応する検索キーワードを前記通信用暗号鍵Ｋｓで暗号化して情報センタ２に送信する（Ｓ５）。

【００３２】情報センタ２では、情報処理装置１ａから検索キーワードを受信すると、検索部２４によって、受信した検索キーワードに対応するディジタル情報をデータベース部２５から検索し、暗号化部２６によって、検索抽出したディジタル情報を前記通信用暗号鍵Ｋｓで暗号化し、さらに認証子Ｎａを計算して付与した後、これらを情報処理装置１ａに送信する（Ｓ６）。

【００３３】情報処理装置１ａは、受信したディジタル情報並びに認証子Ｎａを情報蓄積部１４に蓄積する。ここで、認証子Ｎａは、受信されたディジタル情報の内容の改ざんを検出するためのチェックデータであり、通信用暗号鍵Ｋｓで暗号化されたディジタル情報に対して例えばＭＡＣ（詳細は、ＩＳＯ９７９７参照）等のデータ改ざん検出用認証子作成方法により情報センタ２で計算して付与される。この時、認証子Ｎａの作成用鍵として共通鍵Ｋａが用いられているので、本情報処理装置の操作者が改ざんを検出されない様に情報内容を変更することは困難となる。

【００３４】情報処理装置１ａの操作者が情報を利用する際には、情報処理装置１ａ内において利用対象となるディジタル情報の認証子Ｎａ’が計算され、該認証子Ｎａ’と情報センタ２から直接受信した認証子Ｎａとが比較される。この比較の結果、両者が一致した場合にのみ、情報処理装置１ａの復号部１５で、前記ディジタル情報を復号し、変換出力部１６で情報内容に応じた形態に変換して出力が行われる。

【００３５】前述のように、共通暗号鍵方式を用いた認証、及び暗号化したディジタル情報の通信を行うことにより、通信相手の特定が可能になると共に、通信途中での盗聴防止が可能となる。さらに、情報処理装置１ａにおいて受信したディジタル情報を情報蓄積部１４からそのままコピーして他の装置等で復号及び変換出力しても、本来の意図する情報は復元されないので、不正コピーを防止することができる。また、受信したディジタル情報に認証子Ｎａを付与しているので、受信情報を改ざんした場合、共通鍵Ｋａを知らない限り、利用時の検証で改ざん検出がなされ、情報を復号して変換出力することができず改ざん防止が可能となる。これにより、著作権者並びに情報提供者の権利及び利益を保護することができる。

【００３６】次に、情報処理装置１ａにおいて一度受信したディジタル情報を複数の情報処理装置で利用する場合の手順を図５及び図６に基づいて説明する。図５は、情報処理装置１ａによってディジタル情報を受信する時に、他の情報処理装置１ｂ、１ｃでも利用することを前提に通信する例を示している。

【００３７】まず、情報処理装置１ａ側では、前述したと同様の手順により情報センタ２により認証を受けると共に、通信用暗号鍵Ｋｓの受信を行う。

【００３８】即ち、情報処理装置１ａ側から情報センタ２に発信して、共通鍵蓄積部１１より抽出した情報処理装置１ａの装置番号ＩＤａ及びパスワードＰＡＳＳａを情報センタ２に送信する（ＳＰ１）。情報センタ２で

は、前記受信した装置番号ＩＤａ及びパスワードＰＡＳＳａを共通鍵群管理部２１で検索し、該装置番号ＩＤａ及びパスワードＰＡＳＳａが存在し且つこれらの組み合わせが一致した場合に、乱数Ｒを生成して情報処理装置１ａに返送する（ＳＰ２）。

【００３９】情報処理装置１ａは、乱数Ｒを受信した後、認証データ作成部１３において受信した乱数Ｒを共通鍵蓄積部１１より抽出した共通鍵Ｋａによって暗号化し、暗号化した乱数Ｋａ（Ｒ）を情報センタ２に送信する（ＳＰ３）。

【００４０】情報センタ２では、認証部２３において、共通鍵群管理部２１より抽出した情報処理装置１ａに対応する共通鍵Ｋａで前記乱数Ｒを暗号化すると共に、該暗号化した乱数Ｒの値と受信した暗号化乱数Ｋａ（Ｒ）の値とを照合する。この照合の結果、両者の値が一致した場合には、通信用暗号鍵Ｋｓを生成すると共に、該通信用暗号鍵Ｋｓを情報処理装置１ａに対応する共通鍵Ｋａで暗号化し、暗号化した通信用暗号鍵Ｋａ（Ｋｓ）を情報処理装置１ａに送信する（ＳＰ４）。

【００４１】次に、情報処理装置１ａは暗号化した通信用暗号鍵Ｋａ（Ｋｓ）を受信した後、これを復号して通信用暗号鍵Ｋｓを復元する。この後、情報処理装置１ａから検索したいディジタル情報に対応する検索キーワード、及び情報を利用したい他の情報処理装置１ｂ，１ｃの装置番号ＩＤｂ，ＩＤｃを前記通信用暗号鍵Ｋｓで暗号化して情報センタ２に送信する（ＳＰ５）。

【００４２】情報センタ２では、情報処理装置１ａから検索キーワード及び装置番号ＩＤｂ，ＩＤｃを受信すると、検索部２４によって、受信した検索キーワードに対応するディジタル情報をデータベース部２５から検索して、暗号化部２６によって前記通信用暗号鍵Ｋｓで暗号化し、さらに認証子Ｎａを計算して付与した後、これらを情報処理装置１ａに送信する（ＳＰ６）。

【００４３】次いで、情報センタ２では、先に情報処理装置１ａから受信した装置番号ＩＤｂ，ＩＤｃに対応する共通鍵Ｋｂ，Ｋｃによってそれぞれ暗号化した前記通信用暗号鍵Ｋｓと、共通鍵Ｋｂ，Ｋｃで作成した認証子Ｎｂ，Ｎｃとを組合わせて情報処理装置１ａに送信する（ＳＰ７）。

【００４４】情報処理装置１ａ側では、前記受信した通信用暗号鍵Ｋｓで暗号化されたディジタル情報、並びに各情報処理装置１ｂ，１ｃに対応する共通鍵Ｋｂ，Ｋｃで暗号化された通信用暗号鍵Ｋｂ（Ｋｓ），Ｋｃ（Ｋｓ）及び認証子Ｎｂ，Ｎｃを対応する情報処理装置１ｂ，１ｃの情報蓄積部１４に複写する（ＳＰ８）。

【００４５】このときの複写方法は、情報処理装置１ａと他の情報処理装置１ｂ，１ｃとをケーブル接続してダウンロードする方法、またはフロッピーディスク、光ディスク等のパッケージ媒体経由で複写する方法等がある。複写先の情報処理装置１ｂ，１ｃでのディジタル情報の復号並びに変換出力の手順は、先に説明した情報処理装置１ａでの方式と同様である。

【００４６】次に、情報処理装置１ａの単独利用として受信し、情報処理装置１ａの情報蓄積部１４に蓄積されているディジタル情報を、他の情報処理装置１ｂ，１ｃで利用するための情報処理装置１ａと情報センタ２との間の通信及び操作手順を図６に基づいて説明する。

【００４７】まず、情報処理装置１ａ側では、前述したと同様の手順により情報センタ２により認証を受けると共に、通信用暗号鍵Ｋｓ’の受信を行う。

【００４８】即ち、情報処理装置１ａ側から情報センタ２に発信して、共通鍵蓄積部１１より抽出した情報処理装置１ａの装置番号ＩＤａ及びパスワードＰＡＳＳａを情報センタ２に送信する（ＳＱ１）。情報センタ２では、前記受信した装置番号ＩＤａ及びパスワードＰＡＳＳａを共通鍵群管理部２１で検索し、該装置番号ＩＤａ及びパスワードＰＡＳＳａが存在し且つこれらの組み合わせが一致した場合に、乱数Ｒを生成して情報処理装置１ａに返送する（ＳＱ２）。

【００４９】情報処理装置１ａは、乱数Ｒを受信した後、認証データ作成部１３において受信した乱数Ｒを共通鍵蓄積部１１より抽出した共通鍵Ｋａによって暗号化し、暗号化した乱数Ｋａ（Ｒ）を情報センタ２に送信する（ＳＱ３）。

【００５０】情報センタ２では、認証部２３において、共通鍵群管理部２１より抽出した情報処理装置１ａに対応する共通鍵Ｋａで前記乱数Ｒを暗号化すると共に、該暗号化した乱数Ｒの値と受信した暗号化乱数Ｋａ（Ｒ）の値とを照合する。この照合の結果、両者の値が一致した場合には、通信用暗号鍵Ｋｓ’を生成すると共に、該通信用暗号鍵Ｋｓ’を情報処理装置１ａに対応する共通鍵Ｋａで暗号化し、暗号化した通信用暗号鍵Ｋａ（Ｋｓ’）を情報処理装置１ａに送信する（ＳＱ４）。

【００５１】次に、情報処理装置１ａは暗号化した通信用暗号鍵Ｋａ（Ｋｓ’）を受信した後、これを復号して通信用暗号鍵Ｋｓ’を復元する。この後、情報処理装置１ａによって先に検索したディジタル情報を一意に同定する情報識別番号及び、情報を利用したい他の情報処理装置１ｂ，１ｃの装置番号ＩＤｂ，ＩＤｃを通信用暗号鍵Ｋｓ’で暗号化し、さらに、先の通信で使用した通信用暗号鍵Ｋｓを情報処理装置１ａの共通鍵Ｋａで暗号化した結果を情報センタ２に送信する（ＳＱ５）。

【００５２】この結果、情報センタ２は、先に送信した装置番号ＩＤｂ，ＩＤｃに対応する共通鍵Ｋｂ，Ｋｃでそれぞれ暗号化した前記通信用暗号鍵Ｋｓと、共通鍵Ｋｂ，Ｋｃで作成した認証子Ｎｂ，Ｎｃとの組み合わせを情報処理装置１ａに送信する（ＳＱ６）。

【００５３】次いで、情報処理装置１ａ側では、先に受信した通信用暗号鍵Ｋｓで暗号化されたディジタル情報と、今回受信した各情報処理装置１ｂ，１ｃに対応する

共通鍵Ｋｂ，Ｋｃで暗号化された通信用暗号鍵Ｋｂ（Ｋｓ），Ｋｃ（Ｋｓ）、及び認証子Ｎｂ，Ｎｃを、対応する情報処理装置１ｂ，１ｃの情報蓄積部１４に複写する（ＳＱ７）。

【００５４】このときの複写方法も前述と同様であり、複写先の情報処理装置１ｂ，１ｃでのディジタル情報の復号並びに変換出力の手順は、先に説明した情報処理装置１ａでの方式と同様である。

【００５５】次に、情報処理装置１ａの単独利用として受信し、情報処理装置１ａの情報蓄積部１４に蓄積されているディジタル情報を、他の情報処理装置１ｂで利用する際の、情報処理装置１ｂと情報センタ２との間の通信及び操作手順を図７に基づいて説明する。

【００５６】まず、情報処理装置１ａで受信した暗号化されているディジタル情報を情報処理装置１ｂの情報蓄積部１４に複写する（ＳＲ１）。この後、情報処理装置１ｂを情報センタ２に接続して、前述したと同様の手順により情報センタ２により認証を受けると共に、通信用暗号鍵Ｋｓ’の受信を行う。

【００５７】即ち、情報処理装置１ｂ側から情報センタ２に発信して、共通鍵蓄積部１１より抽出した情報処理装置１ｂの装置番号ＩＤｂ及びパスワードＰＡＳＳｂを情報センタ２に送信する（ＳＲ２）。情報センタ２では、前記受信した装置番号ＩＤｂ及びパスワードＰＡＳＳｂを共通鍵群管理部２１で検索し、該装置番号ＩＤｂ及びパスワードＰＡＳＳｂが存在し且つこれらの組み合わせが一致した場合に、乱数Ｒを生成して情報処理装置１ｂに返送する（ＳＲ３）。

【００５８】情報処理装置１ｂは、乱数Ｒを受信した後、認証データ作成部１３において受信した乱数Ｒを共通鍵蓄積部１１より抽出した共通鍵Ｋｂによって暗号化し、暗号化した乱数Ｋｂ（Ｒ）を情報センタ２に送信する（ＳＲ４）。

【００５９】情報センタ２では、認証部２３において、共通鍵群管理部２１より抽出した情報処理装置１ｂに対応する共通鍵Ｋｂで前記乱数Ｒを暗号化すると共に、該暗号化した乱数Ｒの値と受信した暗号化乱数Ｋｂ（Ｒ）の値とを照合する。この照合の結果、両者の値が一致した場合には、通信用暗号鍵Ｋｓ’を生成すると共に、該通信用暗号鍵Ｋｓ’を情報処理装置１ｂに対応する共通鍵Ｋｂで暗号化し、暗号化した通信用暗号鍵Ｋｂ（Ｋｓ’）を情報処理装置１ｂに送信する（ＳＲ５）。

【００６０】次に、情報処理装置１ｂは暗号化した通信用暗号鍵Ｋｂ（Ｋｓ’）を受信した後、これを復号して通信用暗号鍵Ｋｓ’を復元する。この後、情報処理装置１ａによって先に検索したディジタル情報を一意に同定する情報識別番号と情報処理装置１ａの装置番号ＩＤａとを該通信用暗号鍵Ｋｓ’で暗号化すると共に、情報処理装置１ａで受信した先の通信で使用した通信用暗号鍵Ｋｓを情報処理装置１ａの共通鍵Ｋａで暗号化し、これらの値Ｋｓ’（情報識別番号），Ｋｓ’（ＩＤａ），Ｋａ（Ｋｓ）を情報センタ２に送信する（ＳＲ６）。

【００６１】この結果、情報センタ２は、情報処理装置１ｂの共通鍵Ｋｂで暗号化した前記通信用暗号鍵Ｋｓと共通鍵Ｋｂで作成した認証子Ｎｂを情報処理装置１ｂに送信する（ＳＲ７）。これにより、情報処理装置１ｂにおいて情報処理装置１ａが受信したディジタル情報を使用することができる。

【００６２】前述したように、改ざん防止用認証子を付与したディジタル情報を共通鍵暗号方式での暗号通信により受信し、利用時に認証子による改ざん検証して適合した場合のみ復号、変換して出力しているので、受信したディジタル情報をそのままコピーして他の装置等で復号、変換出力しても、本来の意図する情報は復元されず、不正コピーを防止することができる。

【００６３】また、一度受信したディジタル情報を複数利用者の異なる装置で利用したい場合、複数の装置固有の共通鍵で暗号化した通信用鍵および認証子情報のみを受信し、情報量の多いディジタル情報本体を複製して合法的に利用することができるので、著作者、情報提供業者の権利、利益を損なうことがないと共に、情報量の膨大なディジタル情報を利用する情報処理装置の数だけ繰り返して通信する必要がなく、通信コストの低減及び利用者数の拡大を図ることができる。

【００６４】

【発明の効果】以上説明したように本発明の請求項１によれば、共通鍵暗号方式で通信相手を確認し、認証子付きのディジタル情報を暗号通信により授受し、利用時に認証子を検証して適合した場合のみ復号、変換出力しているため、通信相手の確実な同定、通信途中での盗聴防止が可能となる。さらに、受信したディジタル情報をそのままコピーして他の装置等で復号、変換出力しても、本来の意図する情報は復元されず、不正コピーを防止できる。また、受信情報に認証子を付与することにより、受信情報を改ざんした場合も、共通鍵を知らない限り、利用時の検証により改ざん検出し、復号、変換出力しない機構になっており、改ざん防止も可能となる。また、ディジタル情報蓄積部に蓄積された受信情報をそのままコピーして保存しておき、利用時に再度同一のディジタル情報処理装置のディジタル情報蓄積部に戻してから、復号、変換出力して利用することができるため、ディジタル情報蓄積部の蓄積容量制限以上に受信しても外部記憶装置に保存しておくことができる。また、ディジタル情報蓄積部のファイルの人為的でない物理的破壊等に備えてのバックアップコピーとしても機能するという大きな効果がある。これらの結果、著作者及び情報提供業者の権利並びに利益を保護することができる。

【００６５】また、請求項２によれば、上記の効果に加えて、一度受信したディジタル情報を他の複数の情報処理装置での合法的利用が可能になり、情報量の膨大なデ

ィジタル情報を利用する情報処理装置の数だけ繰り返して通信する必要がなく、通信コストの低減及び利用者数の拡大を図ることができ、この結果、著作者及び情報提供業者の権利保護並びに利益拡大に貢献することができる。

【００６６】また、請求項３によれば、上記の効果に加えて、任意の情報処理装置によって受信したディジタル情報を必要時に応じて他の情報処理装置で使用することができる。

【００６７】さらに、請求項４によれば、上記の効果に加えて、任意の情報処理装置によって受信したディジタル情報を他の情報処理装置で使用する際に、該他の情報処理装置と情報センタとの通信によって、該他の情報処理装置において前記ディジタル情報を合法的に使用することができ、利用手続の簡単化を図ることができるという非常に優れた効果を奏するものである。

【図面の簡単な説明】

【図１】本発明の一実施例におけるディジタル情報通信システムを示す構成図

【図２】一実施例における共通鍵蓄積部内の情報内容例を示す図

【図３】一実施例における共通鍵群管理部内の情報内容例を示す図

【図４】一実施例における情報処理装置と情報センタとの間での通信手順を説明する図

【図５】一実施例における情報処理装置と情報センタとの間での通信手順及び他の情報処理装置への複写手順を説明する図

【図６】一実施例における情報処理装置と情報センタとの間での通信手順及び他の情報処理装置への複写手順を説明する図

【図７】一実施例における情報処理装置と情報センタとの間での通信手順及び他の情報処理装置への複写手順を説明する図

【符号の説明】

１…情報処理装置、１１…共通鍵蓄積部、１２…通信制御部、１３…認証データ作成部、１４…情報蓄積部、１５…復号部、１６…変換出力部、２…情報センタ、２１…共通鍵群管理部、２２…通信制御部、２３…認証部、２４…検索部、２５…データベース部、２６…暗号化部、３…通信路。

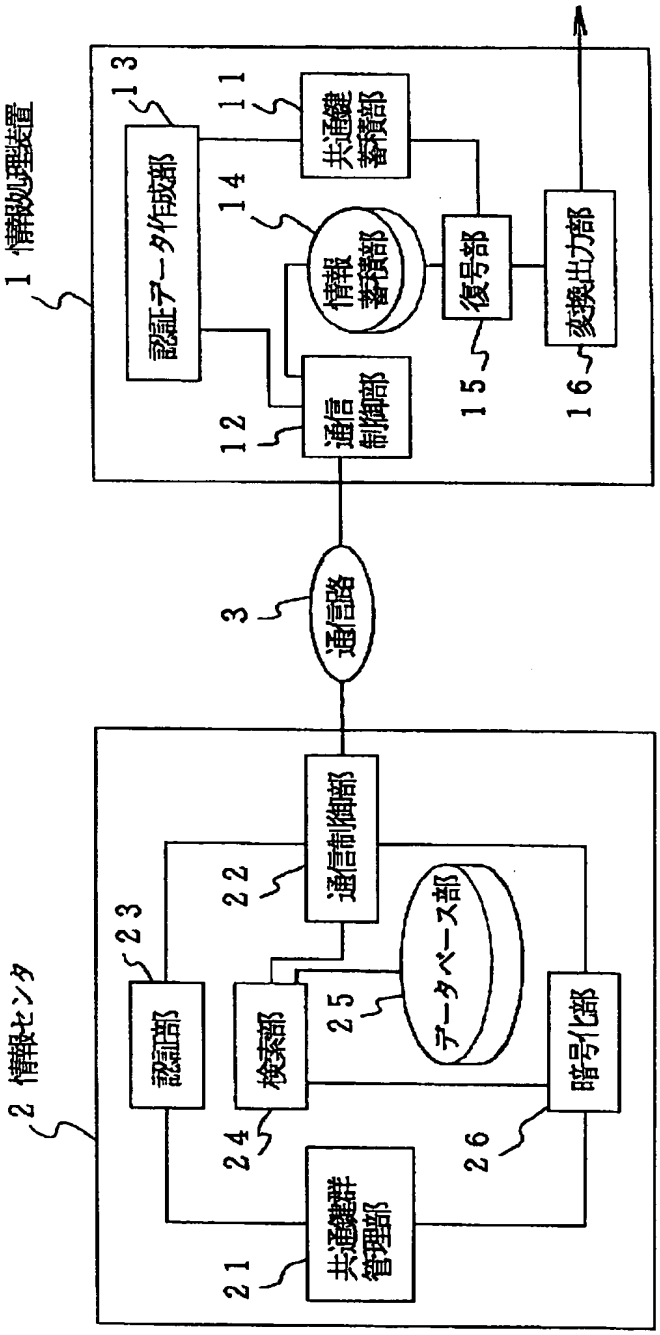
【図２】

IDa	PASSa	Ka

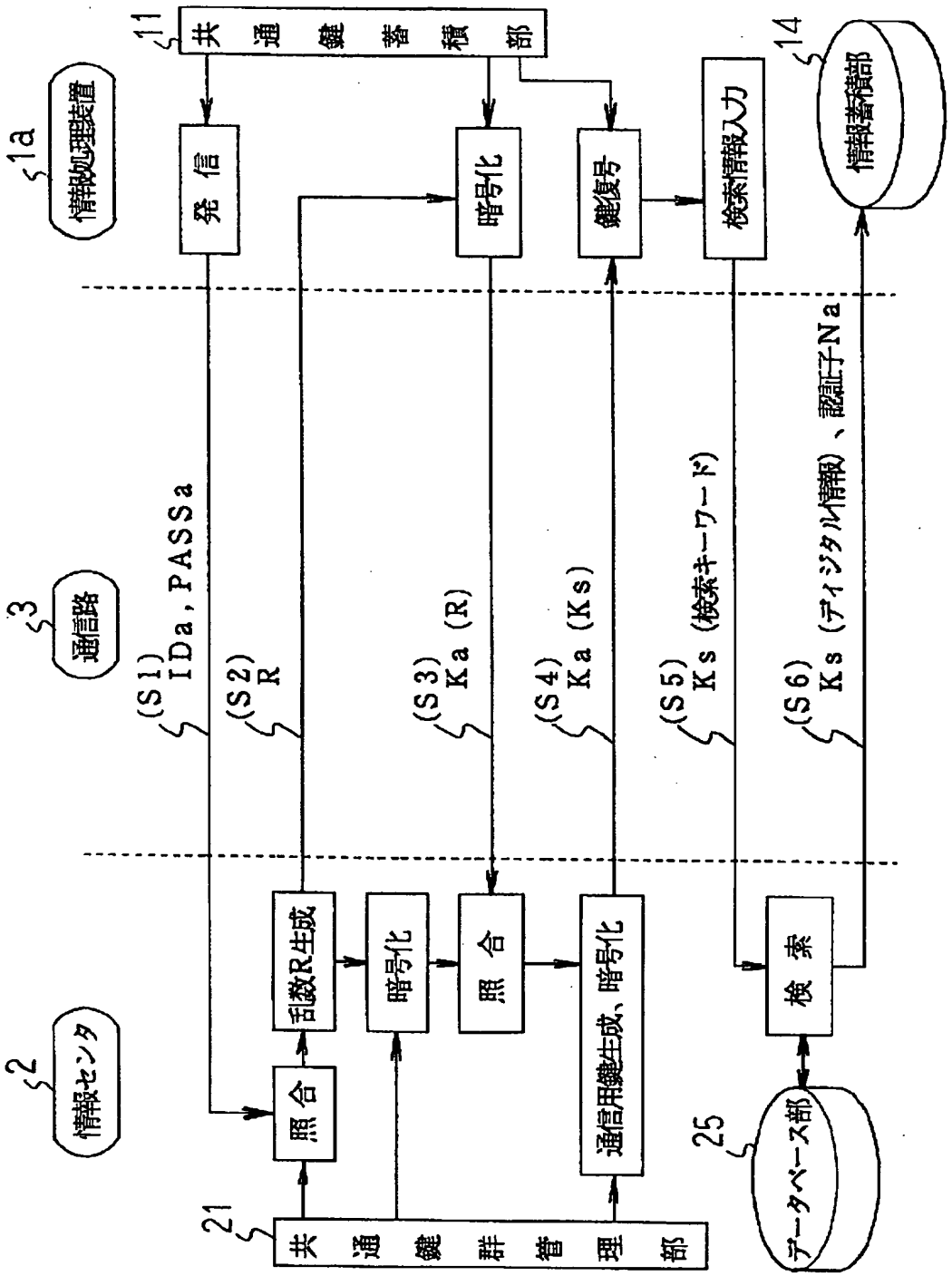
【図３】

IDa	PASSa	Ka
IDb	PASSb	Kb
IDc	PASSc	Kc
...	.....	..

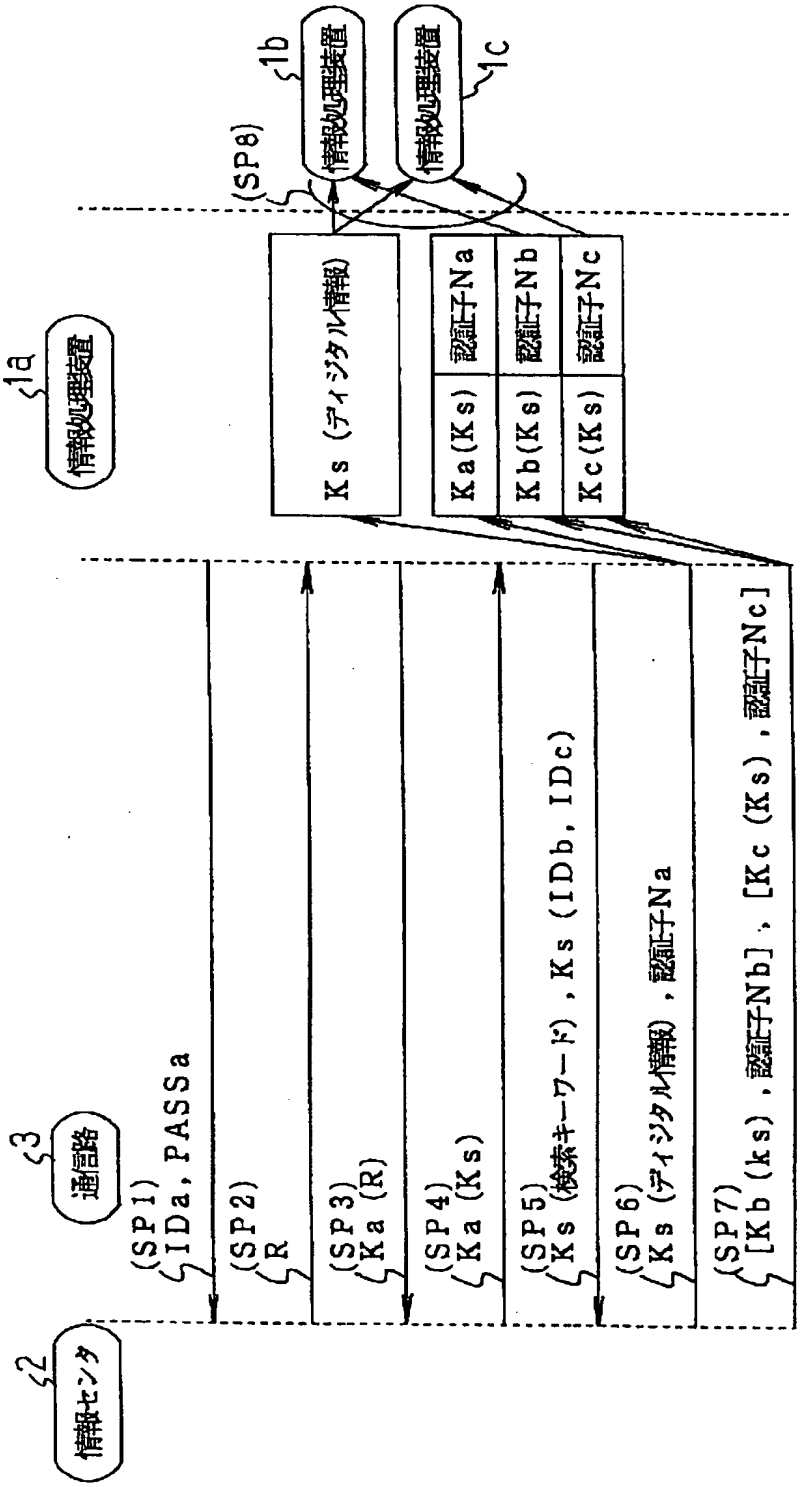
【図１】


１ 情報処理装置
１３
１１
認証データ作成部
共通鍵蓄積部
１４
情報蓄積部
復号部
変換出力部
１２
通信制御部
１５
１６
３
通信路
２ 情報センタ
２３
２２
通信制御部
認証部
検索部
２５
データベース部
暗号化部
２４
２６
２１
共通鍵群管理部

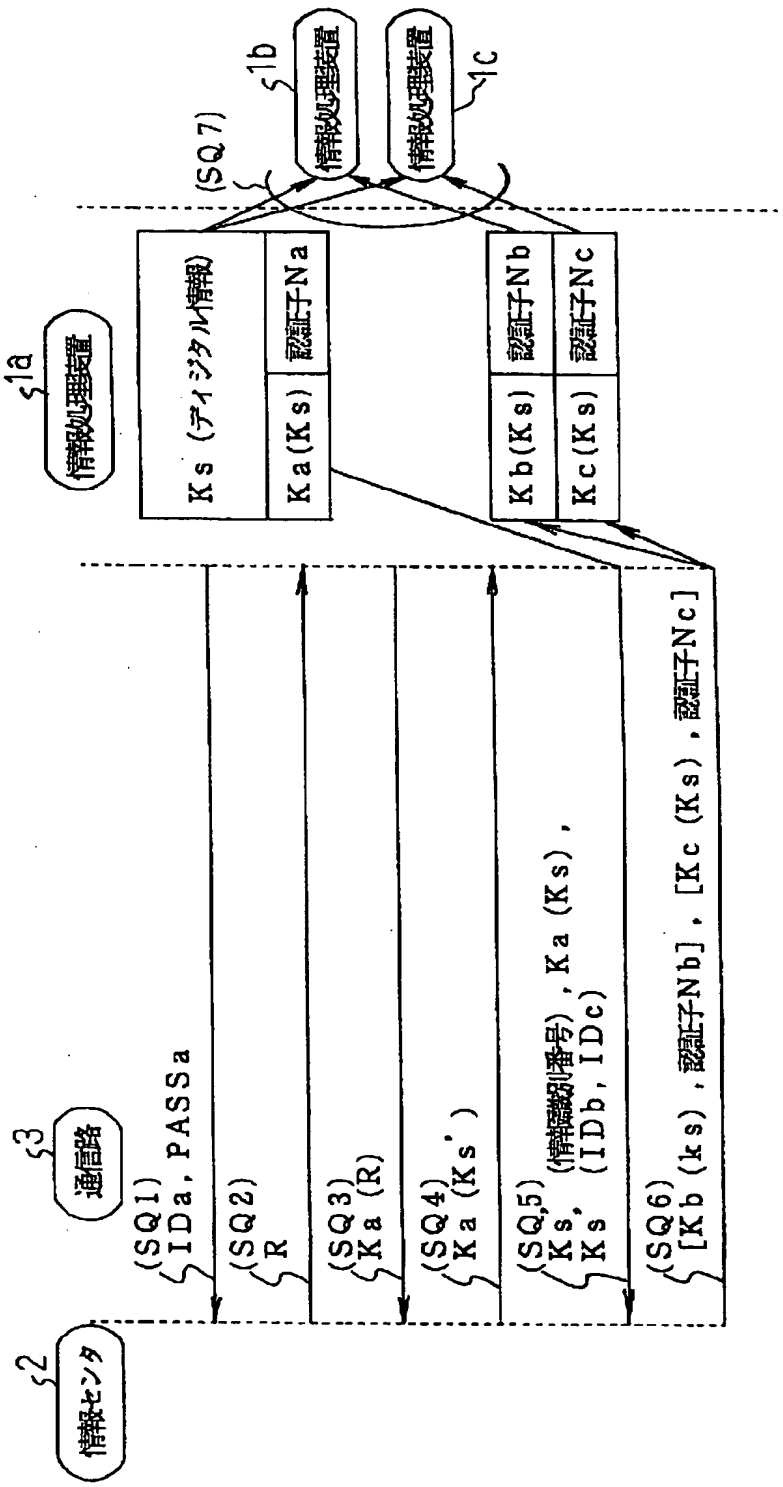
【図４】


情報処理装置
1a
共通鍵蓄積部
11
発信
暗号化
鍵復号
検索情報入力
情報蓄積部
14
通信路
3
(S1) IDa, PASSa
(S2) R
(S3) Ka (R)
(S4) Ka (Ks)
(S5) Ks (検索キーワード)
(S6) Ks (ディジタル情報)、認証子Na
情報センタ
2
乱数R生成
暗号化
照合
照合
通信用鍵生成、暗号化
検索
共通鍵群管理部
21
データベース部
25

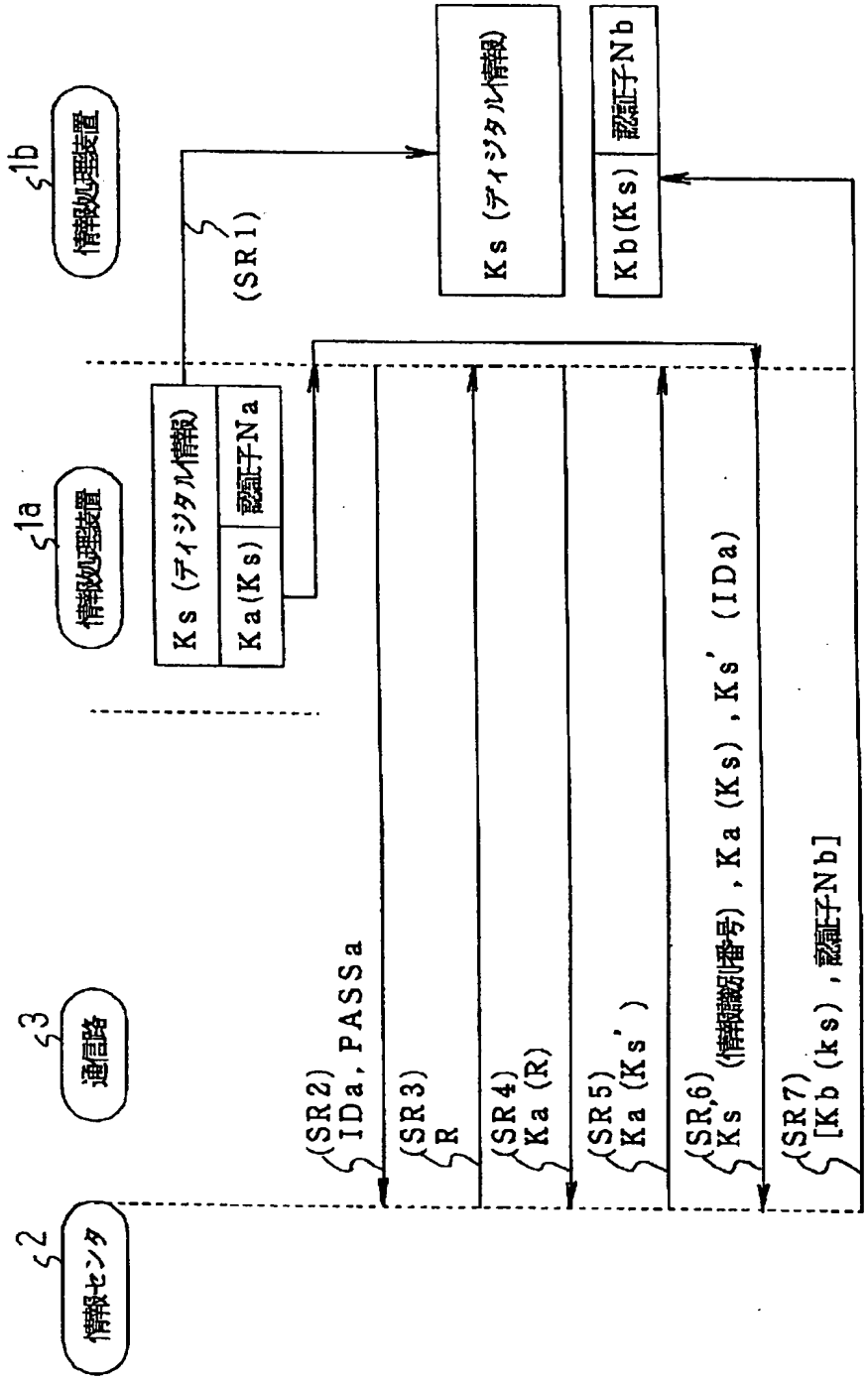
【図5】


情報センタ
通信路
情報処理装置
情報処理装置
情報処理装置
(SP1) IDa, PASSa
(SP2) R
(SP3) Ka (R)
(SP4) Ka (Ks)
(SP5) Ks (検索キーワード), Ks (IDb, IDc)
(SP6) Ks (ディジタル情報), 認証子Na
(SP7) [Kb (ks), 認証子Nb], [Kc (Ks), 認証子Nc]
(SP8)
Ks (ディジタル情報)
Ka(Ks)
認証子Na
Kb(Ks)
認証子Nb
Kc(Ks)
認証子Nc

【図６】


情報センタ
2
通信路
3
情報処理装置
1a
情報処理装置
1b
情報処理装置
1c
(SQ7)
Ks (ディジタル情報)
Ka(Ks)
認証子Na
Kb(Ks)
認証子Nb
Kc(Ks)
認証子Nc
(SQ1)
IDa, PASSa
(SQ2)
R
(SQ3)
Ka (R)
(SQ4)
Ka (Ks')
(SQ,5)
Ks', (情報識別番号), Ka (Ks),
Ks' (IDb, IDc)
(SQ6)
[Kb (ks), 認証子Nb], [Kc (Ks), 認証子Nc]

【図７】



フロントページの続き

(51)Int.Cl.⁶	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		9364－5L		